ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ МОЛДОВА

Александра НИЧИПУРЕНКО

Департамент социально-гуманитарных наук, SI-234,Факультет Вычислительной Техники, Информатики и Микроэлектроники, ТУМ, Кишинев, Молдова

Автор кореспондент: Александра НИЧИПУРЕНКО, e-mail: alexandra.nicipurenco@isa.utm.md

Научный координатор **Наталья КЭРБУНЕ**, профессор социально-гуманитарных наук, UTM

Аннотация. *Несмотря на все те блага, которые были внесены современными технологиями в жизнь человека, нельзя игнорировать возникновение и распространение такого феномена, как киберпреступность. Это означает, что совершение преступлений в киберпространстве должно предполагать такую же серьезную уголовную ответственность, как и нарушение закона в реальной жизни. Целостность и защита информации как элементов критической инфраструктуры, так и каждого гражданина в отдельности напрямую зависит от уровня развития области информационной безопасности государства. С какими кибернетическими угрозами столкнулись граждане Республики Молдова и какие меры были предприняты правительством для их предотвращения? В ходе исследования этого вопроса выяснилось, что, учитывая принятие законов, проектов и поправок к Уголовному Кодексу страны, в Республике Молдова наблюдается тенденция к росту числа киберпреступлений и нарушений в информационной среде. Проведение курсов, тренингов, направленных на цифровую грамотность населения и профилактику инцидентов, работа над законодательными нормами и улучшение государственного контроля в сфере информационной безопасности могут стать одним из решений по борьбе с киберпреступлениями в Республике Молдова.*

Ключевые слова: *кибербезопасность, угрозы, киберпреступления, меры по борьбе*

Введение

В XXI веке наряду со стремительным развитием информационных технологий стала возникать острая необходимость в усовершенствовании подходов к анализу угроз, рисков, уязвимостей в информационном обществе и обеспечении информационной безопасности, как индивидуальных пользователей, предприятий, бизнеса, критической инфраструктуры, включая здравоохранение, энергетическую, транспортную и банковскую структуры, так и национальной безопасности, военной инфраструктуры и обороны.

В настоящее время на глобальном уровне киберпреступления происходят с увеличивающейся частотой, приобретая более сложные и масштабные формы, принося при этом значительный ущерб как государственным, так и частным секторам, а также гражданским лицам. Несанкционированный доступ к сетям и услугам электронных коммуникаций, неавторизированное изменение, удаление или повреждение информационных данных, нелегальное ограничение доступа к этим данным и кибершпионаж – проблемы мирового уровня. Угрозы и риски, атаки и кибернетические инциденты, а также другие события, происходящие в киберпространстве, материализуются путем использования уязвимостей человеческого, технического и процедурного характера. Экономические потери вследствие подобных уязвимостей весьма существенны.

Первостепенной задачей информационной безопасности и специалистов, действующих в этой области, является разработка новых и эффективных методов решения этих проблем и предотвращения их в будущем.

Актуальность

Актуальность информационной безопасности в Республике Молдова, как и во всем мире, возрастает с каждым днем. В современном информационном обществе, где компьютеры, сети и интернет играют ключевую роль во всех аспектах нашей жизни, кибербезопасность становится неотъемлемой частью нашей повседневной деятельности. Информационная безопасность или кибербезопасность в Республике Молдова находит свое применение в таких областях, как бизнес и предпринимательство, государственные организации, здравоохранение, финансы, образование и личная жизнь граждан. Информационная безопасность во всех этих областях призвана выполнять функцию защиты конфиденциальной информации, медицинских, банковских, персональных данных и образовательных ресурсов, предупреждать мошенничества и кибератаки, вести борьбу с кибершпионажем и кибертерроризмом.

Определить степень подготовленности государства к обеспечению информационной безопасности можно с помощью глобального индекса кибербезопасности (ГИК), который является одним из показателей, измеряющих степень приверженности стран кибербезопасности на глобальном уровне. Специалисты оценивают информационную безопасность любой из стран мира по пяти критериям: юридическая, техническая, организационная подготовленность, готовность к сотрудничеству, развитие образовательного и исследовательского потенциала страны [1]. Согласно мировому рейтингу ГИК на 2020 год Республика Молдова занимает 71 строку [2]. Самой кибербезопасной страной является США, а в 10-ку лидеров входят: Великобритания, Саудовская Аравия, Эстония, Республика Корея, Сингапур, Испания, Российская Федерация. Исходя из Global Security Map, Республика Молдова занимает 4-е место среди 242 других стран в зависимости от индекса кибербезопасности, набирая 238,1 по шкале от 0 до 1000 баллов [3].

В настоящее время вопросы кибербезопасности государства приобретают особую значимость в связи с тем, что кибератаки наносят экономический ущерб, подрывают доверие общества к онлайн-сервисам и наносят реальный вред гражданам, их имуществу и конфиденциальности. Они происходят в основном из-за человеческой халатности и безответственности, таких как ненадежные пароли, утечки личных данных [4]. Злоумышленники в киберпространстве используют разнообразные инструменты и методы для проведения кибератак и атак на информационные системы и данные, используя вирусы, программы-вымогатели, троянцы, шпионское ПО, ботнеты, рекламное ПО, SQL-инъекции, атаки Man-in-the-Middle, DDoS-атаки, фишинг и другие виды мошенничества [5].

В последние несколько десятилетий Республика Молдова предприняла ряд мер по предотвращению и борьбе с информационной преступностью. Одним из наиболее значимых событий было подписание Конвенции в Будапеште 2001 года, которое состоялось 23 ноября 2001 года и было ратифицировано Законом № 6 от 2 февраля 2009 года. Конвенция вступила в силу для Республики Молдова 1 сентября 2009 года. Сразу после ратификации Конвенции в Будапеште был принят Закон № 20 от 3 февраля 2009 года о предотвращении и борьбе с информационной преступностью. Этот закон регулирует юридические отношения, связанные с:

a) предупреждением и борьбой с преступностью в сфере компьютерной информации;

b) системой взаимопомощи в области предупреждения и борьбы с преступностью в сфере компьютерной информации, защиты и оказания помощи поставщикам услуг и пользователям компьютерных систем;

c) сотрудничеством органов публичного управления с неправительственными организациями, другими представителями гражданского общества в деятельности по предупреждению и борьбе с преступностью в сфере компьютерной информации;

d) сотрудничеством с другими государствами, международными и региональными организациями, компетентными в данной области [6]. В этот же период произошли изменения в Главе XI "Информационные преступления и преступления в области

телекоммуникаций" Уголовного кодекса Республики Молдова, предусматривающие ответственность за совершение преступлений в области информатики и электросвязи. Данная глава включает четыре статьи: 259 (Несанкционированный доступ к компьютерной информации), 260 (Внесение или распространение вредоносных компьютерных программ), 261 (Нарушение правил безопасности информационных компьютерных систем), 261/1 (Несанкционированный доступ к сетям или услугам электросвязи) [7].

Несмотря на существующие законы, в Республике Молдова ежегодно происходят преступления в области информатики и электросвязи. Согласно информации из Автоматизированной информационной системы «Регистр криминалистической и криминологической информации», предоставленной Министерством внутренних дел, начиная с 2013 года и до августа 2015 года включительно, было зарегистрировано 72 информационных преступления по статьям 208 и 259-261 Уголовного кодекса Республики Молдова, с материальным ущербом в размере около 21588 тысяч леев. В тот же самый период времени было зарегистрировано 57 нарушений авторского права и смежных прав на общую сумму наложенных штрафов приблизительно 99 тысяч леев [8].

По данным исследования Business Software Alliance (BSA) 2018 года, относительно незаконного использования программного обеспечения для персональных компьютеров, Республика Молдова вошла в группу стран с самым высоким уровнем пиратства в регионе Центральной и Восточной Европы. Армения лидировала в регионе с самой высокой долей нелицензионного программного обеспечения на уровне 85 процентов, за ней следовали Молдова с 83 процентами и Беларусь с 82 процентами [9].

Одним из крупнейших преступлений в области информационной безопасности в Республике Молдова стало преступление, зарегистрированное в банковском секторе. В течение 2013 года подсудимые обвинялись в том, что предлагали изменение номеров мобильных операторов в Республике Молдова по сниженным ценам, составляющим 50-70% от стоимости операции. Кроме того, подсудимые содействовали приобретению GSM-оборудования, информационных систем и других электронных средств по сниженным ценам на некоторых онлайн-сервисах. Для совершения этих операций были использованы данные иностранных банковских карт без ведома и согласия их владельцев для совершения транзакций на сумму более 250 000 молдавских лей [10].

Исходя из всего вышесказанного, можно констатировать, что в Республике Молдова наблюдается тенденция к росту числа киберпреступлений и нарушений в сфере информационной безопасности. В связи с этим в 2018 году Генеральная прокуратура в сотрудничестве с Министерством внутренних дел разработала законопроект № 161, получивший название «Big Brother», основная цель которого заключалась в том, чтобы привести молдавские законы в соответствие с международными стандартами, установленными Конвенцией о киберпреступности. Генеральный прокурор Республики Молдова на период с 8 декабря 2016 — 11 июля 2019 Эдуард Харунжен отметил, что электронные обыски, перехват информационных данных и другие идентичные меры, предусмотренные в этом законопроекте, используются в многочисленных странах. По словам генпрокурора, такого рода вмешательство допустимо только при крайней необходимости, в строго обусловленных угрозами обстоятельствах, в случае особо тяжких преступлений. «При этом не считается, что они могут повлечь какие-либо риски нарушения права на частную жизнь. Соответствующие действия сопровождаются гарантиями соблюдения фундаментальных прав и свобод человека. Эти механизмы включены и в проект закона *Big Brother*». Несмотря на сопротивление, с которым столкнулся данный законопроект, в настоящее время при внесении определенных поправок, включая аспект соблюдения пропорциональности вмешательства государства в частную жизнь граждан, он в полной мере соответствует международным стандартам и помогает в раскрытии социально опасных деяний и защите граждан от преступности. «Каждое государство, обеспечивая национальную безопасность, должно самостоятельно оценивать риски, которым оно

подвергается, и создавать собственные механизмы противостояния этим рискам», - подчеркнул генеральный прокурор Эдуард Харунжен [11].

К приоритетным направлениям и мерам, содействующим эффективности борьбы с цифровыми преступлениями в Республике Молдова, можно отнести работу над законодательными нормами, улучшение государственного контроля в данной сфере, а также проведение курсов, тренингов, направленных на профилактику инцидентов информационной безопасности и грамотности населения в этой области.

Выводы

В наше время современные технологии влияют на все сферы нашей повседневной жизни, однако они также делают нас более уязвимыми перед лицом случайных и намеренных киберугроз. В Республике Молдова, как и во многих других странах, информационные системы и данные становятся объектом интереса для киберпреступников. Нападения на информационные системы могут привести к серьезным последствиям, включая утечку конфиденциальных персональных данных, финансовые потери, нарушение процессов в бизнесе, а также угрозы национальной безопасности. По этой причине не следует недооценивать важность обеспечения кибербезопасности в Республике Молдова.

Обеспечение информационной безопасности не только национального уровня, но и отдельных граждан имеет большое значение, так как цифровые угрозы могут затронуть как государственные структуры, так и личные интересы людей. С учетом постоянно меняющейся природы киберугроз, постоянное совершенствование и адаптация подходов к информационной безопасности являются неотъемлемой частью современного мира. Таким образом, информационная безопасность – это область, которая требует постоянного улучшения, осведомленности и развития в Республике Молдова.

Библиографический список источников:

[1] О. П. Советникова, «Информационная безопасность и киберпреступления в Республике Беларусь», Беларусь, p.1000, 2021.
[2] «Global Cybersecurity Index 2020.» [Online]. Available: https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/#:~:text=In%202020%2C%20the%20United%20States,score%20of%2099.54%20for%20each
[3] „Global Security Map” [Online]. Available: https://globalsecuritymap.com/
[4] O. Melnyk, «Current aspects of cyber security», Узбекистан, pp.45-46, 2022.
[5] „Что такое кибербезопасность?” [Online]. Available: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security
[6] Закон № 20 от 03-02-2009 о предупреждении и борьбе с преступностью в сфере компьютерной информации, Республика Молдова.
[7] Codul penal al Republicii Moldova, Capitolul XI «Infracţiunile în domeniul informaticii şi reţelelor electronice», Республика Молдова.
[8] Постановление о Национальной программе кибербезопасности Республики Молдова на 2016-2020 годы № 811 от 29.10.2015, Республика Молдова.
[9] «Software Management: Security Imperative, Business Opportunity BSA Global Software Survey» ,p. 12, Jun. 2018.
[10] I. Pascar, «Criminalitatea informatică în Republica Moldova», Республика Молдова, pp. 277-278, 2015.
[11] „Digital Report” [Online]. Available: https://digital.report/generalnyiy-prokuror-moldovyi-segodnya-usiliya-po-borbe-s-kiberprestupnostyu-stali-prioritetom/